UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728

7590 01/25/2007

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/972,371	IWAMURA, RYUICHI	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 17-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 17-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 01 December 2006 have been fully considered but they are not persuasive. Applicant argues that Johnston cannot meet the limitation of a "digital media device" merely because it involves telephone voice communications. This argument is not persuasive because voice communications over the system are in a digital format (Col. 1, line 13), and voice communications are certainly a form of audio media.

2. Applicant argues that Johnston does not disclose a "receiving device" because the device in Johnston is not primarily functioned to receive. This argument is not persuasive because Applicant is trying to import meaning into the claims outside of the actual claim language. The claims merely recite a "receiving device", and a cellular phone receives data.

3. Applicant's argument that Johnston does not disclose "encrypting said digital signal" because the encryption is Johnston is done for transmission, is not persuasive because the claim merely requires "a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit." The claim is silent with respect to the ultimate path of the encrypted digital signal. Therefore, Johnston's disclosure of a cellular phone encrypting digital voice signals meets the claim limitation. Applicant's correlation of the cellular phone of Johnston to a "transmitter" is not persuasive because as previously stated; cellular telephones are capable of transmission and reception. Therefore, a cellular telephone can clearly be considered "a receiver."

4. Applicant's argument that "Johnston actually teaches decryption of a received signal (column 11, lines 4-5), in contrast to Claim 17 that recites encryption of a received signal," is not

persuasive because this simply is not the case. Claim 17 mere requires "a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit." No mention is made as to the source of the digital signal.

Applicant's argument that "Johnston fails to teach or fairly suggest the limitation, 'a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory'," is not persuasive because Johnston disclose that the SIM cards are reprogrammable so that they may be tailored to specific communication environments (Col. 16, lines 47-49), which meets the limitation of modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory (From the Office Action mailed 01 September 2006). Applicant's citation and analysis of (column 1, lines 36-37) of Johnston is misplace and irrelevant to the anticipation rejection of claim 19.

5. Examiner respectfully asserts that Applicant's understanding of Johnston (Col. 16, lines 47-49) is incorrect. Johnston does not disclose "replacement of SIM cards to enable secure communication among a group", but actually disclose, "all user terminals are provided with reprogrammed SIM cards to allow secure communication within the temporary group (word-for-word from Johnston)." Reprogramming a SIM cannot be considered "replacement" in any reasonable way.

6. In response to applicant's argument that Spies teaches away from the claimed invention, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must

be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

7. In response to applicant's argument that the proposed combination would change the principle operation of at least one of the references, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). The modification is **only** to encrypt the decryption key in the IC card, with the public key of the set top box, prior to transmitting the decryption key to the set top box. One of ordinary skill in the art at the time the invention was made would have been motivated to make such a modification so that the decryption key can only be accessed (decrypted in this case) by the set top box (using the set top box specific private key) in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

8. Applicant argues that the principle operation of Deo is changed if the PIN requirement was removed. This argument is irrelevant to the rejection of claim 1, because the Office Action is silent with respect to removal of the PIN requirement in Deo.

9. In response to applicant's argument that Deo is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977

F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Deo is reasonably pertinent to the problem of cryptography when it comes to protecting data.

10. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., point of deployment security module (POD)) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

11. Applicant's argues that a third piece of art, which is not cited, has been introduced to reject claim 6. This is simply not the case. Page 7 of the Office Action mailed on 01 September 2006, shows that claims 1 and 3-7 are rejection under 103(a) as being unpatentable over Spies. in view of Deo. The actual rejection of claim 6 is on page 10 of that same Office Action, with no mention of any additional art. Spies is the only piece of prior art even mentioned with respect to the rejection of claim 6.

12. Applicant continues to argue that Spies does not disclose "MPEG compliant signals." This argument is not persuasive because Spies discloses a secure video content delivery system (Figure 6 & Abstract & Col. 11, lines 40-42). This video content is distributed to users over satellite networks (Col. 1, line 21) or on DVDs (Col. 1, line 24). Video content distributed over satellite networks and encoded on DVDs is in one format, and one format only, **MPEG** (See the previously presented evidence document MPEG Handbook, pages 368-369 & 390). Therefore, because Spies discloses that the video is distributed via satellite networks or DVDs, the limitations involving the MPEG format are met.

13. Applicant argues that "The MPEG Handbook", which was presented as rebuttal evidence (as requested by Applicant), does not qualify as prior art. This is irrelevant because "The MPEG Handbook" is not being used as a prior art reference. "The MPEG Handbook" was introduced as rebuttal evidence. Applicant requested evidence supporting the Examiner's initial position that mere teaching of video distribution through satellite network and DVD means, inherently included teaching of the MPEG format. The only date requirement for rebuttal evidence is that the evidence be published prior to the argument for which the evidence is relied upon to rebut.

14. Applicant appears to confuse the rationale presented by the Examiner with respect to the teaching in Spies of video distribution via satellite networks and DVDs. Examiner did not take the position that "all digital video is MPEG encoded", as alleged by Applicant. Instead, the Examiner stated that all video distributed over satellite networks and DVDs is encoded using MPEG (See paragraph 6 on pages 4-5) of the previous Office Action. Therefore, since Spies specifically recites that the digital video data is distributed over satellite networks or DVDs, the limitation of MPEG encoding in inherent to that teaching.

15. Applicant attempt to disqualify any statements of inherency by alleging that "Audio Video Interleave ('AVI') encoding is widely used in the taught 'on-line networks'," is not persuasive because although AVI formatting may be use in **on-line networks**, it is **not** used in satellite networks or DVDs. Therefore, the teaching of MPEG encoding is still inherent to **satellite networks and DVDs**.

16. In response to applicant's argument that Spies teaches away from embodiments of the present invention with respect to Diffie-Hellman, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary

reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Claim Rejections - 35 USC § 102

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

18. Claims 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Johnston, U.S. Patent No. 6,373,946. Referring to claim 17, Johnston discloses a communication security system wherein a mobile handset terminal (Figure 2) comprises a terminal processor (Figure 2, element 37) and a SIM card (Figure 2, element 35). The mobile handset terminal meets the limitation of the digital media receiving device. The SIM card meets the limitation of a first logical circuit, and the terminal processor meets the limitation of the second logical circuit. The SIM card receives a partial key that is used to generate an encryption key (Col. 10, lines 36-43, 52-53 & Col. 11, lines 14-17). The SIM card supplies this encryption key to the terminal processor to encrypt data (Col. 10, lines 51-53), which meets the limitation of a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit. Prior to transmitting the encryption key to the terminal processor, the SIM card decrypts the partial key that is ultimately used to generate the encryption key (Col. 12, lines 20-

24), which meets the limitation of a first logical circuit for decrypting a local encryption key. The SIM card contains a processor (Figure 2, element 35a) and a memory (Figure 2, element 35b & Col. 6, lines 20-23), which meets the limitation of said first logical circuit comprising a local processor and local memory.

Referring to claim 18, Johnston discloses that the SIM card stores an encryption algorithm to decrypt data (Col. 12, lines 8-12), which meets the limitation of a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

Referring to claim 19, Johnston discloses that the SIM cards are reprogrammable so that they may be tailored so specific communication environments (Col. 16, lines 47-49), which meets the limitation of a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

Referring to claim 20, Johnston discloses that the data stored in the SIM cannot be read or accessed (Col. 1, lines 36-37), which meets the limitation of the contents of said local memory cannot be observed from outside of said first logical circuit.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

21. Claims 1, 3-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781. Referring to claim 1, Spies discloses a secure video content delivery system wherein an IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of generating a public encryption key. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10), which meets the limitation of in a digital media receiving device, accessing an encrypted signal at said first logical circuit, determining a first decryption key for said encrypted signal at said logical circuit, at said first logical circuit decrypting said encrypted signal using said first decryption key. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from

the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 3, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55), which meets the limitation of accessing a computer control program for a second portion of local of local memory at said second logical circuit. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be

decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claims 4, 5, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). The IC card functionality can be updated or changed (Col. 12, lines 1-4), which meets the limitation of replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 6, Spies discloses that the cryptographic functions can be updated by replacing DLLs (Col. 12, lines 1-4), which meets the limitation of accessing a second decryption

key from a first portion of local memory at said first logical circuit, replacing a computer control program stored in a second portion of local memory at least first logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory, and executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

Referring to claim 7, Spies discloses that the video content can be TV broadcasts (Col. 1, lines 14-29), which are transmitted in MPEG format.

22. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781 as applied to claim 1 above, and further in view of Schneier. Referring to claim 2, Spies does not disclose using Diffie-Hellman algorithm for key exchange. Schneier discloses using the Diffie-Hellman algorithm for public key exchange (Pages 513-514). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in the secure video content delivery system of Spies because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100